A mathematical model for ascertaining the same ciphertext generated from distinct plaintext in the Michael O. Rabin Cryptosystem

Md. Shamim Hossain Biswas*

* Department of Software Engineering, Daffodil International University, Bangladesh

DOI: 10.14299/ijser.2019.06.08
https://doi.org/10.14299/ijser.2019.06.08

Abstract— The aim of this research is to overcome the ambiguity of the Michael O. Rabin Cryptosystem. Because the Rabin cryptosystem often generates the same ciphertext from different plaintexts as well as multiple plaintexts from a single ciphertext, this problem arises from modular reduction arithmetic. Separating a particular ciphertext from the same type of ciphertext generated from different plaintexts is quite cumbersome. If the question arises as to how to distinguish a particular ciphertext against every plaintext, to answer the question, this paper presents a new mathematical model that generates a specific ciphertext for each plaintext. This mathematical model is actually a symmetric cipher because it is able to encrypt and decrypt messages with a symmetric key. The model consists of three algorithms: key generation, encryption, and decryption. The Diffie-Hellman key exchange protocol is used for key generation. The encryption depends on the floor value of the quadratic quotient and the quadratic residue. The decryption relies on computing the absolute value of the square root of an expression that multiplies the key with the floor value of the quadratic quotient and adds the quadratic residue. The advantage of the proposed model is that the intended receiver gets only one plain value, distinguishing the ciphertext against the plaintext. The idea came to mind while reviewing a research article called Michael O. Rabin Cryptosystem. Computational and exploratory research approaches were applied in this research. Data collection methods were a literature review, an online survey questionnaire, and a focus group discussion. The population of this research work was university professors.

Index Terms—Cryptography, Cryptosystem, Encryption, Decryption, Diffie-Hellman key exchange protocol, Euclidean algorithm.

1 Introduction

Cryptosystem is usually consist of a several of algorithms: key generation, encryption, and decryption algorithms.

The security of a cryptosystem mainly relies on a secret key. Michael O. Rabin Cryptosystem was the first asymmetric cryptosystem in the field of public-key cryptography. The security of Rabin's encryption mechanism relies on prime integer factorization. Since its publication in January 1976 and 1979 by Michael O. Rabin, a huge number of surveys have been carried out over Rabin's cryptosystem to find out its efficiency and devise a new method for a real-life application [1, 2]. It was not widely used due to some ambiguity; however, its theoretical significance is widespread. The encryption mechanism used quadratic residue to produce cipher text, and decryption was accomplished by computing two square roots and Bezout's coefficient using the extended Euclidean algorithm and combining them with the Chinese remainder theorem. Similarly to the RSA and ElGamal cryptosystems, the Michael O. Rabin cryptosystem is described in a ring under addition and multiplication modulo a composite integer number. One of the main disadvantages is that it generates four results during decryption, and extra effort is needed to sort out the right one out of the four possibilities. In addition to that, Rabin's cryptosystem often generates the same ciphertext from different plaintexts. This is one of the limitations that arise in modular reduction arithmetic. Thus, the motivation for conducting research on this topic is to overcome the ambiguity of Rabin's cryptosystem. For this reason, it is necessary to design a new mathematical model to overcome the ambiguity. To do that, this research paper is going to show a new mathematical model based on the Diffie-Hellman key exchange protocol [3], the concept of square modular arithmetic, a square root, floor function, and absolute value. This idea originated from a research gap identification period, particularly when reviewing Rabin's cryptosystem. In the beginning, designing a mathematical model that could efficiently separate each ciphertext from each plaintext was quite cumbersome. Of course, continuous effort gets the task accomplished. In the proposed cryptosystem, the encryption is done by hashing the message twice, i.e., $C = (H_1 = m^2 \bmod K,\ H_2 = \lfloor m^2 / K \rfloor)$, and decryption is done by $(D) = \left| \sqrt{H_2 * K + H_1} \right|$. The advantage of this cryptosystem is that the intended receiver gets only one desired plaintext with this technique, whereas Rabin's cryptosystem generates four different decryption results. This research outcome is very significant for the field of cryptography.

The next road map of the article is organized as follows: Section 2 contains a literature review; Section 3 proposes a mathematical model; Section 4 provides discussion; Section 5 gives a conclusion; Section 6 gives acknowledgement; and the last section provides references as well as an appendix as a reference for ASCII value.

2 LITERATURE REVIEW

The literature review section provides a thorough discussion of Michael O. Rabin's cryptosystem and the contributions made by other researchers to it. First of all, let us start with an overview of Rabin's cryptosystem [4]. In this system, to establish a secret communication between two entities, one of the entities creates a public key with its corresponding private key in the following way and then encrypts and decrypts the message:

Algorithm for Key generation: Entity A ought to take the subsequent actions in order to generate public key:

1. Generate two large and distinct random prime numbers p and q, each roughly the same size.
2. Compute N = p ∗ q as her public key

Algorithm for Rabin's public-key encryption: When entity B encrypts a message(m) for entity A, entity B should perform the following steps:

1. Obtain A's authentic public key N.
2. Represent the message as an integer m: $\{0, 1 \ldots n-1\}$
3. Compute ciphertext $(c) = m^2 \ mod \ N$.
4. Send the ciphertext to A.

Algorithm for Rabin public-key Decryption: To recover plaintext(m) from ciphertext (c), A must locate the four-square roots of c modulo n— m_1, m_2, m_3, and m_4. One of the values of the four-square roots—m_1, m_2, m_3 and m_4—will be the sending message. A determines which of the four-square roots is m by identifying the bits that replicate in the following way:

1. Use the extended Euclidean algorithm to find integers Y_p and Y_q satisfying expression $p.Y_p + q.Y_q = 1$.
2. Compute $M_p = c^{(p+1)/4} \bmod p$.
3. Compute $M_q = c^{(q+1)/4} \bmod q$.
4. Compute $x = (Y_p.p.M_q + Y_q.q.M_p) \bmod N$.
5. Compute $y = (Y_p.p.M_q - Y_q.q.M_p) \bmod N$.
6. The four-square roots are $+x, -x, +y$ and $-y \bmod N$.

To better understand this mathematical concept, let's now look at an example of the aforementioned algorithm. In the key generation step, an entity A chooses two prime numbers $p = 277$, and $q = 331$, and generates public key $N = p * q = 91687$. In the encryption process, the last six bits of original messages must be replicated prior to encryption. In order to encrypt the 10-bit message (m) = 1001111001, B replicates the last six bits of the original message (m) to obtain the 16-bit message (m) = 1001111001111001, which in decimal notation is (m) = 40569. The entity B then computes $(C) = m^2 \bmod N = 405692 \bmod 91687 = 62111$ and sends this to the entity A. In the decryption Process, A uses the aforesaid algorithm and her knowledge of the factors of N to compute the four-square roots of C mod N: $m_1 = 69654, m_2 = 22033, m_3 = 40569$, and $m_4 = 51118$. Its binary format is $m_1 = 10001000000010110$, $m_2 = 101011000010001$, $m_3 = 1001111001111001$, and $m_4 = 1100011110101110$. Entity A decrypts c to m_3 and recovers the original message (m) = 100111100 because because only m_3 possesses the necessary redundancy.

Now let us examine an additional mathematical interpretation of Rabin's cryptosystem. It consists of three steps: encryption, decryption, and key setup. During the key generation phase, Alice chooses two random prime numbers, P and Q to use as her private keys. She then multiplies the two private keys to get the public key, i.e., (N) = P ∗ Q. Additionally, she picks a random integer number $(0 \leq b < N)$ to publicize (N, b) as her public key. In the encryption process, Bob, the sender generates cipher text using an expression, i.e., $C = m\ (m + b)\ mod\ N$. In this case, b is only used for security purposes. In the decryption step, Alice solves the quadratic equation $m^2 - m * b + c \equiv 0\ (mod\ N)$ to decrypt the ciphertext. The decryption involves computing square roots modulo N. Decryption consisting of $m^2 \equiv a\ (mod\ N)$. This is performed by solving the expression, i.e., $M_p = m^2 \equiv a\ (mod\ p)$ and $M_q = m^2 \equiv a\ (mod\ q)$, picking a random integer b in the range of $0 \ldots . p$ and then computing the Legendre symbol $(b^2 - 4a)\ /p$ i.e., $(b^2 - 4a)^{(P-1)/2}\ mod\ p$ with result $p - 1$ replaced by -1, until that's -1. Now setup the second-degree polynomial arithmetic *f*, and then compute the polynomials $x^{(p+1)/2}\ mod\ f$, and $x^{(q+1)/2}\ mod\ f$ using polynomial arithmetic modulo the polynomial *f*. Compute Bezout's coefficient using the extended Euclidean algorithm, and then combine these results with the Chinese remainder theorem to arrive at four possible solutions in most cases and pick the right one in some way.

Let us see an example. ***In the first step***, calculate the public key $(N) = p * q = 1273$ by choosing two random prime numbers: $p = 41$ and $q = 53$. Then, assume a message $(m) = 92$. Calculate ciphertext $(c) = m^2\ mod\ N = 1945$. Now compute $M_p = m^2 \equiv a(mod\ p) = 18$ and $M_q = m^2 \equiv a(mod\ q) = 37$. ***In the second step***, select a random number $b = 2$ satisfying the condition and set up a polynomial $f = x^2 - b * x + M_p$ with coefficients in Z_{41}, that is $f = x^2 + 39x + 18$. Similarly, let's set $b = 4$ satisfying the condition and set up a polynomial $f = x^2 + 49x + 37$ with coefficients in Z_{53}

https://doi.org/10.14299/ijser.2019.06.08

where x is the variable of the polynomial and has no particular value. ***In the third step***, compute the polynomial $x^{\frac{p+1}{2}} \bmod f = x^{21} \bmod f$. The binary representation of the exponential order (21) is 10101, and compute $x^2, x^4, x^5, x^{10}, x^{20}$ and finally x^{21} mod f by left-to-right binary exponentiation. Computation of $x^2 \bmod f \Longrightarrow x^2 - (x^2 + 39x + 18) \Longrightarrow 2x + 23$. Computation of $x^4 \bmod f$ that is $4x^2 + 10x + 37 - 4(x^2 + 39x + 18) = 18x + 6$. Computation of $x^5 \bmod f \Longrightarrow 18x^2 + 6x - (x^2 + 39x + 18) \Longrightarrow \mathrm{x} + 4$. Computation of $x^{10} \bmod f$ that is $(x + 4)^2 \bmod f \Longrightarrow 10x + 39$. Computation of $x^{20} \bmod f$ that is $(10x + 39)^2 \bmod f \Longrightarrow 37x + 8$. Computation of $x^{21} \bmod f$ that is $37x^2 + 8x \bmod f$. Finally, the x term has surprised by leaving 31. Thus, $m^2 \equiv a(mod\ p)$ has solution $M \in \{10, 31\}(mod\ p)$. ***In the fourth step***, compute the polynomial $x^{\frac{q+1}{2}} \bmod f$ that is $x^{27} \bmod f$ using polynomial arithmetic modulo the polynomial f. The binary representation of the exponential order (27) is 11011, and compute $x^2, x^3, x^6, x^{12}, x^{13}, x^{26}$ and finally $x^{27} \bmod f$ by left-to-right binary exponentiation. Then apply similar computation as like as ***third step*** and then solve $m^2 \equiv a\ (mod\ q)$, with solution $M \in \{14, 39\}(mod\ q)$. ***In the fifth step***, compute Bezout's coefficient using the extended Euclidean algorithm: $Y_p = 22, Y_q = -17$. ***In the sixth step***, the computation of four roots: $R_1 = \left(Y_p.p.M_{q_1} + Y_q.q.M_{p_1}\right) mod\ N = 728$, $R_2 = -R_1\ mod\ N = 1445$, $R_3 = \left(Y_p.p.M_{q_2} - Y_q.q.M_{p_2}\right) mod\ N = 2081$, and $R_4 = -R_3\ mod\ N = 92$. Thus, using the Chinese remainder theorem yields the four possible outcomes: $\{728, 1445, 2081, 92\}$.

Let's move on to the discussion about the Diffie-Hellman key exchange protocol. It was the first public-key algorithm to be published. It appears in the seminal paper by Diffie and Hellman that established public-key cryptography [5]. The protocol for exchanging keys is commonly known as the Diffie-Hellman protocol. A number of commercial products employ this key exchange technique. The Diffie-Hellman key exchange protocol enables two users to securely exchange a key for subsequent encryption and decryption of messages. The algorithm is only capable of exchanging secret values. The effectiveness of the Diffie-Hellman key exchange protocol relies on the difficulty of computing discrete logarithms, which is widely regarded as a difficult problem. The following is a discussion of the Diffie-Hellman key exchange protocol:

Global public elements*:** q is a prime number that can define a domain so called curve area or elliptic curve, α is a primitive root of q such that α < q. ***Key generation for user A: Select a private key X_a , such that $X_a < q$. Calculate the public key $Y_a = \alpha^{x_a}\ mod\ q$. ***Key generation for user B:*** Select a private key X_b such that $X_b < q$. Calculate the public key $Y_b = \alpha^{x_b}\ mod\ q$. ***Secret key for user A:*** $K = (Y_b)^{x_a}\ mod\ q$. ***Secret key for user B*:** $K = (Y_a)^{x_b}\ mod\ q$.

As an illustration, consider the domain size $(q) = 353$ and its primitive root $(\alpha) = 3$. Two users (A and B) select secret keys A = 97 and B = 233, respectively. Each of them computes a public key. For example, user A computes $X = 3^{97}\ mod\ 353 = 40$ and user B computes $Y = 3^{233}\ mod\ 353 = 248$. Following that, they exchange public keys with one another to compute secret keys in the following ways: A computes $K = (Y)^A\ mod\ 353 = 248^{97}\ mod\ 353 = 160$.
B computes $K = (X)^B\ mod\ \ 353 = 40^{233}\ mod\ 353 = 160$.
There have been many surveys dedicated to Rabin's cryptosystem. Recent scientific journals have published numerous updates to Rabin's cryptosystem. Let's examine its further variations.

Hayder Raheem Hashim [6] proposed an update methodology that used three private keys instead of two. One ciphertext results in eight non-deterministic plaintexts, whereas one of them is the actual plain text. This technique has the advantage of confusing attackers while being very annoying to receivers because it requires extra effort to distinguish the original plaintext from the eight texts.

Yahia Awad et al. [7] proposed a deterministic method based on the Gaussian integer domain to choose the correct plaintext among four decryption results. The recipient can decide on a particular plaintext from four possible decryption results by selecting the obtained square root with redundancies in its imaginary part. This is the main benefit of using the Gaussian integer technique. However, the drawback is that modular reduction arithmetic can generate the same ciphertext from different plaintexts. For example, for the four plaintexts $(m) = \{13, 20, 57, 64\}$, we get the same ciphertext $(c) = 15$.

Manish Bhatt et al. [8] extended a deterministic technique by adding duplicated bits at the beginning of plain text before encrypting it. One of the four possible decryption results reflects the replicating bits. The other three false results, which relate to memory complicity and time complexity, are annoying to the receiver.

Masahiro Kaminaga et al. [9] discussed a fault attack technique on modular exponentiation during Rabin's encryption, where a complicated situation arose in the case of message reconstruction when the message and public key were not relatively prime. They also provided a rigorous algorithm to handle message reconstruction.

Haytham Gani [10] performed a study on the Rabin and RSA cryptosystems and provided an insightful discussion. Both Rabin's cryptosystem and RSA computed at about the same speed. Both algorithms' security relies on prime integer factorization.

Preeti Chandrakar [11] discussed a secure two-factor remote authentication scheme using the Rabin Cryptosystem. This paper showed an extended usage of Rabin's cryptosystem. Xue-dong DONG et al. [12] modified Rabin's cryptosystem

https://doi.org/10.14299/ijser.2019.06.08

using the cubic residue technique, which successfully removed the long-cherished inconsistency of the so-called four-to-one function in Rabin's cryptosystem. However, the authors noted that it was insecure against the chosen cipher text attack. It's interesting to note that the novel method for calculating the cubic root from a cubic residue keeps a private key secret.

My research focuses on constructing a symmetric-key cryptosystem by providing a solution to overcome the ambiguity of the Michael O. Rabin Cryptosystem using mathematical concepts derived from a literature review that analyzed other people's findings in various contexts of Rabin's cryptosystems and their varieties.

A. AIMS AND OBJECTIVES

The goal of the research is to overcome the ambiguity of Rabin's cryptosystem and develop a cryptographic technique that can encrypt and decrypt messages using a semmetric key. And therefore, the following research questions have been formulated from the research objectives to conduct this study:

RESEARCH QUESTIONS

1. What is the obfuscation of the Michael O. Rabin Cryptosystem?
2. How do I design a mathematical model to over come the ambiguities of the Rabin cryptosystem?

3 PROPOSED MATHEMATICAL MODEL

3.1 Key generation model:

Diffie-Hellman Key Exchange protocol

$$K = (Y_b)^{xa} \bmod N$$
$$= (\alpha^{xb} \bmod N)^{Xa} \bmod N$$
$$= (\alpha^{xb})^{Xa} \bmod N$$
$$= \alpha^{xb \,.\, Xa} \bmod N$$
$$= (\alpha^{Xa})^{xb} \bmod N$$
$$= (\alpha^{Xa} \bmod N)^{Xb} \bmod N$$
$$= (Y_a)^{xb} \bmod N$$

Author Contribution

3.2 Encryption model:

$H_1 =$ m^2 mod K
$H_2 = \lfloor m^2 / K \rfloor$
$C = (H_1, H_2)$, where C = Ciphertext.
$H_1 =$ Quadratic residue and
$H_2 =$ Floor value of quadratic quotient

3.3 Decryption model:

$D = \left|\sqrt{H_2 * K + H_1}\right|$

4 DISCUSSIONS

The proposed cryptographic technique ensures secure communication between two parties. At the initial stage, Alice and Bob create a shared secret key using the Diffie-Hellman key exchange protocol, for example. In the second stage, Bob chooses a message $A = 065$ according to the ASCII binary character table [13]. ASCII is a character-encoding standard for electronic communication. It represents text on a computer, telecommunications equipment, and other devices. Note that details about ASCII codes are available on the internet. After selecting an ASCII value, Bob encrypts the message like a pair of integers using a shared secret key and sends it to Alice. Finally, Alice decrypts the message. The following is the entire mathematical procedure for deciphering a message:

Step 1: Key generation process:

Alice		Evesdroper		Bob	
known	un-known	known	unknown	Known	un-known
N=113		✓		✓	
$G = 5$		✓		✓	
P = 7	Q = 11		P = 7 Q = 11	Q = 11	P = 7
$A = 5^7(113) = 42$		Dynamic		$B = 5^{11}(113) = 34$	
$A = 34^7(113) = 40 = k_a$		Swapping		$B = 42^{11}(113) = 40 = k_b$	

Step 2: Encryption Process:

In the encryption step, one of the parties encrypts a message using a shared secret key and sends it to other parties. Assume that Bob encrypts the message A = 65 using the shared secret key and sends it to Alice. $H_1 = (65)^2 \bmod 40 = 25$, $H_2 = \lfloor (65)^2/_{40} \rfloor = 105$, C = (105,25)

Step 2: Decryption Process:

In the decryption step, the receiver decrypts the message using a shared secret key. Suppose, Alice receives the message and decrypts it by applying a square root to the result of $(H_2 * K + H_1)$, and only the absolute value is considered for a secret message- $D = \left|\sqrt{H_2 * K + H_1}\right| = \left|\sqrt{105 * 40 + 25}\right| = \left|\sqrt{4225}\right| = 65 = A$ (reveal).

https://doi.org/10.14299/ijser.2019.06.08

4.1 COMPARISON

The comparison between the proposed cryptographic technique and the Michael O. Rabin cryptosystem is as follows:

Rabin's Crypto Scheme:	*Proosed Crypto Scheme:*
It's ciphertext is a quadratic residue.	It's ciphertext is a pair of integers.
Decryption generates four plain texts.	Decryption generates single plaintext.
It uses an asymetric key.	It uses a symetric key.
Michael O. Rabin's encryption and signature scheme cannot identify the same ciphertext generated from different plaintext.	It is powerful due to its ability to distinguish the same ciphertext generated from different plaintexts.

A disadvantage of the Mivhel O. Rabin cryptosystem:

$C = 13^2 \bmod 77 = 15$		$C = 20^2 \bmod 77 = 15$
$C = 57^2 \bmod 77 = 15$		$C = 64^2 \bmod 77 = 15$

The same encryption result (15) gererates from four different plaintexts (m) = {13,20,57,64}. Those encryption results cannot be identified separately by the Rabin cryptosystem.

An advantage of the proposed mathematical model:

$H_1 = (13)^2 \bmod 77$ $H_2 = \lfloor (13)^2/_{77} \rfloor$ $C = (15, 2)$		$H_1 = (20)^2 \bmod 77$ $H_2 = \lfloor (20)^2/_{77} \rfloor$ $C = (15, 5)$
$H_1 = (57)^2 \bmod 77$ $H_2 = \lfloor (57)^2/_{77} \rfloor$ $C = (15, 42)$		$H_1 = (64)^2 \bmod 77$ $H_2 = \lfloor (64)^2/_{77} \rfloor$ $C = (15, 53)$

The proposed technique can identify each ciphertext separately.

5 CONCLUSIONS

The proposed mathematical model is efficient for solving four-to-one mapping ciphertexts. It can efficiently identify each ciphertext separately generated from modular reduction arithmetic, while Rabin's cryptosystem fails. The objective of this research has been successfully achieved.

A. RECOMMENDATION: I welcome cryptographic researchers to come up with new ideas that will be more effective than the current model.

B. LIMITATION: This is a very simple idea in a cryptographic context. This work is for educational purposes only. It may not be useful for professional work.

6 ACKNOWLEDGEMENTS

I am very grateful to my family members who supported me financially to conduct this study because, without their financial support, this work could not be carried out. I thank Md. Maruf Hassan and Dr. Md. Mostafijur Rahman for their inspirational advice. This work was part of the academic curriculum fulfillment for the degree of MSc in software engineering with a major in cybersecurity.

REFERENCES

[1] Michael O Rabin. Probabilistic algorithms algorithms and complex ity: New directions and recent results, *ACADEMIC PRESS, INC. New York San Francisco*, December 1976, pp. 21-40

[2] Michael O Rabin, "Digitized signatures and public key functions as intractable as factorization". *technical report MIT-LCS-TR-212*, MIT laboratory for computer science, 1979.

[3] Bert Den Boer. "Diffie-hellman is as strong as discrete log for certain primes". In: *Conference on the Theory and Application of Cryptography*, pages 530–539. Springer, 1988.

[4] A. Menezes, P. van Oorschot and S. Vanstone. "Michael.O. Rabin cryptosystem". *Handbook of Applied Cryptography*.

[5] William Stallings, *Cryptography and Network Security*, Fourth Edition. Page No.299. Figure 10.7. .e-text ISBN-10: 0-13-187319-9. Publisher: Prentice Hall Pub Date: November 16, 200

[6] Hayder Raheem Hashim. "H-Rabin Cryptosystem". In: *Jounal of Math ematics and Statistics*. 10.3844/jmssp.2014.304.308. Rsearchgate public cation no. 264286919

[7] Yahi Awad, Abdul Nasser El-Kassar, Terrar Kadri. "Rabin's Public-key Cryptosystem in the Domain of Gaussian Integers". In: *interna tional Conference on Computer and application (ICCA), 2018.*

[8] Manish Bhatt Shweta Suman, Maroti Deshmukh*. "DRC_Determin istic_Rabin_Cryptosystem". In: *3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, 2018. Researchgate publication no. 325330795

[9] Masahiro Kaminaga, Hideki Yoshikawa, Member, IEEE, Arimitsu Shikoda, and Toshinori Suzuki. "A Modulus Attack on Modular Squaring for Rabin Cryptosystem". DOI: 10.1109/TDSC.2016.2602352, IEEE Crashing.

[10] Haytham Gani. "a Mathematical Analysis of RSA and Rabin Cryp tosystem". In: *ResearchGate publication no. 332834881*, 2019

[11] Preeti Chandrakar, Hari Om. "An efficient two factorremote user Au thentication and session key agreement scheme using Rabin Cryp tosystem", 2017. In: DOI: 10.1007/s13369-017-2709-6

[12] Xue-dong DONG, Shuo Han and Yun-Feng BAI. "A modifications of the Rabin Cryptosystem based on Cubic Residues". In: *Communica tions, Information Management and Network Security*, 2017 (CIMNS 2017), ISBN: 978-1-60595-498-1

[13] Sticks and Stones. " An alphabet book for the 21st century".

Author Biography

Name: Md. Shamim Hossain Biswas
MSc in Software Engineering (Cybersecurity), Daffodil International University
BSc in Computer Science & Engineering, Stamford University Bangladesh
E-mails: shamim.ak.pico@gmail.com, shamim44-165@diu.edu.bd
ORCID: 0000-0002-4595-1470

https://doi.org/10.14299/ijser.2019.06.08